LISTING OF CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 – 134 (Cancelled)

135. (Currently Amended) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data, excluding the predetermined bits in the digital data, ~~resulting in~~ with the digital signature, the digital data including the inserted associated data;

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data; [[and]]

receiving the associated data from a Global Positioning Satellite transmission;

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature; and

outputting the digital data with the digital signature inserted into the predetermined bits.

136. (Previously Presented) The method of claim 135, wherein the signing step comprises:

applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and encrypting the hash.

137. (Previously Presented) The method of claim 135, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

138. (Previously Presented) The method of claim 135, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

139. (Previously Presented) The method of claim 135, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

140. (Previously Presented) The method of claim 139, wherein the digital data is an image and each sample is an image pixel.

141. (Previously Presented) The method of claim 139, wherein the digital data is video and each sample is a spatial temporal sample.

142. (Previously Presented) The method of claim 139, wherein the digital data is audio and each sample is a time sample.

143. (Previously Presented) The method of claim 139, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

144. (Previously Presented) The method of claim 135, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising the step of transforming the plurality of bits into an alternative representation having at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

145. (Previously Presented) The method of claim 144, wherein the digital data is an image and each sample is an image pixel.

146. (Previously Presented) The method of claim 144, wherein the digital data is video and each sample is a spatial temporal sample.

147. (Previously Presented) The method of claim 144, wherein the digital data is audio and each sample is a time sample.

148. (Previously Presented) The method of claim 144, wherein the associated data is inserted into at least a portion of the second characteristic component.

149. (Previously Presented) The method of claim 148, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

150. (Previously Presented) The method of claim 135, wherein the associated data comprises data identifying a source of the digital data.

151. (Previously Presented) The method of claim 135, wherein the associated data comprises data identifying the identity of an owner of the digital data.

152. (Previously Presented) The method of claim 151, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.

153. (Previously Presented) The method of claim 135, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

154. (Previously Presented) The method of claim 135, wherein the associated data comprises at least two fields.

155. (Previously Presented) The method of claim 154, wherein at least one other field comprises data identifying the owner of the public key.

156. (Previously Presented) The method of claim 135, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step; signing the decompressed file resulting in the digital signature; and

inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

157. (Previously Presented) The method of claim 156, wherein the digital data is an image and the compression standard is JPEG.

158. (Previously Presented) The method of claim 156, wherein the digital data is video and the compression standard is MPEG.

159. (Previously Presented) The method of claim 135, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step;

inserting the associated data into the decompressed file;

signing the decompressed file resulting in the digital signature; and

inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

160. (Previously Presented) The method of claim 159, wherein the digital data is an image and the compression standard is JPEG.

161. (Previously Presented) The method of claim 159, wherein the digital data is video and the compression standard is MPEG.

162. (Previously Presented) The method of claim 135, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the method further comprises the steps of:

ignoring the least significant bit plane in the digital data;

concatenating the associated data to the digital data having the ignored least significant bit plane prior to the signing step;

performing the signing step to the digital data having concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

163. (Previously Presented) The method of claim 135, further comprising the steps of:

providing time data identifying the time the digital data was created;

concatenating the hash and the time data;

applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and

encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

164. (Previously Presented) The method of claim 163, further comprising the steps of:

transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and

receiving the time stamp from the third party prior to the inserting step.

165. (Previously Presented) The method of claim 164, wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

166. (Previously Presented) The method of claim 163, wherein the time stamp is provided by a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the time data which together with the digital signature is signed by the circuit to output the time stamp.

167. (Previously Presented) The method of claim 135, further comprising the steps of:

storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory; and

outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

168. (Previously Presented) The method of claim 167, further comprising the steps of storing a private key for signing the digital data in the memory corresponding to each user and using the private key for signing the digital data.

169. (Previously Presented) The method of claim 167, wherein the recognizing step is accomplished by a fingerprint recognition system.

170. (Previously Presented) The method of claim 167, wherein the identifier is a name of the recognized user.

171. (Currently Amended) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for signing the digital data, excluding the predetermined bits in the digital data, ~~resulting in~~ with the digital signature, the digital data including the inserted associated data;

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data;

means for inserting associated data into the digital data prior to signing the digital data such that the encoder authenticates both the associated data as well as the digital data; and

means for receiving the associated data from a Global Positioning Satellite transmission;

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature and at least a portion of the associated data comprises data identifying the identity of an owner of the digital data.

172. (Previously Presented) The encoder of claim 171, wherein the means for signing comprises:

means for applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and

encrypting the hash.

173. (Previously Presented) The encoder of claim 171, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

174. (Previously Presented) The encoder of claim 171, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

175. (Previously Presented) The encoder of claim 171, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

176. (Previously Presented) The encoder of claim 175, wherein the digital data is an image and each sample is an image pixel.

177. (Previously Presented) The encoder of claim 175, wherein the digital data is video and each sample is a spatial temporal sample.

178. (Previously Presented) The encoder of claim 175, wherein the digital data is audio and each sample is a time sample.

179. (Previously Presented) The encoder of claim 175, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

180. (Previously Presented) The encoder of claim 171, wherein the digital data is an image comprising a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising means for transforming the plurality of bits into an alternative representation having at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

181. (Previously Presented) The encoder of claim 180, wherein the digital data is an image and each sample is an image pixel.

182. (Previously Presented) The encoder of claim 180, wherein the digital data is video and each sample is a spatial temporal sample.

183. (Previously Presented) The encoder of claim 180, wherein the digital data is audio and each sample is a time sample.

184. (Previously Presented) The encoder of claim 180, wherein the associated data is inserted into at least a portion of second characteristic component.

185. (Previously Presented) The encoder of claim 184, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

186. (Previously Presented) The encoder of claim 171, wherein the associated data comprises data identifying a source of the digital data.

187. (Previously Presented) The encoder of claim 171, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.

188. (Previously Presented) The encoder of claim 171, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

189. (Previously Presented) The encoder of claim 171, wherein the associated data comprises at least two fields.

190. (Previously Presented) The encoder of claim 171, wherein at least one of the fields comprises data identifying the owner of the public key.

191. (Previously Presented) The encoder of claim 171, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for signing the decompressed file resulting in the digital signature; and

means for inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

192. (Previously Presented) The encoder of claim 191, wherein the digital data is an image and the compression standard is JPEG.

193. (Previously Presented) The encoder of claim 191, wherein the digital data is video and the compression standard is MPEG.

194. (Previously Presented) The encoder of claim 171, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for inserting the associated data into the decompressed file;

means for signing the decompressed file with the associated data inserted therein resulting in the digital signature; and

means for inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

195. (Previously Presented) The encoder of claim 194, wherein the digital data is an image and the compression standard is JPEG.

196. (Previously Presented) The encoder of claim 194, wherein the digital data is video and the compression standard is MPEG.

197. (Previously Presented) The encoder of claim 171, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the encoder further comprises:

means for ignoring at least a portion of the least significant bit plane in the digital data;

means for concatenating the associated data to the digital data having the ignored least significant bit plane prior to signing the digital data;

means for signing the digital data having the concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

198. (Previously Presented) The encoder of claim 171, further comprising:

means for providing time data identifying the time the digital data was created;

means for concatenating the hash and the time data;

means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and

means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

199. (Previously Presented) The encoder of claim 198, further comprising:

means for transmitting the hash to a third party for providing the time stamp and concatenating the hash and time stamp; and

means for receiving the second hash from the third party prior to encryption.

200. (Previously Presented) The encoder of claim 199, wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

201. (Previously Presented) The encoder of claim 198, further comprising a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the time data which together with the digital signature is signed by the circuit to output the time stamp.

202. (Previously Presented) The encoder of claim 171, further comprising:

a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognition means for recognizing a user of the device whose identifier is stored in the memory; and

output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

203. (Previously Presented) The encoder of claim 202, wherein a private key for signing the digital data is also stored in memory corresponding to each user, wherein the identifier is inserted as associated data and the private key is used to sign the digital data.

204. (Previously Presented) The encoder of claim 203, wherein the recognition means is a fingerprint recognition system.

205. (Previously Presented) The encoder of claim 204, wherein the identifier is a name of the recognized user.